

1 **ENABLING SURVEILLANCE OF NETWORK CONNECTED DEVICES**

2 **FIELD OF THE INVENTION**

3 The present invention relates to theft prevention of personal computers and other similar
4 computer-like devices that are easily removable. It is more particularly concerned with
5 those devices that normally connect to a network e.g., a LAN (Local Area Network),
6 while in use.

7
8 **BACKGROUND OF THE INVENTION**

9 Laptop computers and other similar computer-like devices are getting smaller, lighter and
10 more powerful. What makes them appealing to business people also attracts criminals. If
11 there is nothing as frustrating as losing a word processing document or a spreadsheet file,
12 losing a whole computer to theft and its invaluable content such as highly confidential
13 and sensitive business-critical data may be devastating to an organization. In all surveys
14 about computer crime conducted e.g., by insurance companies or some specialized
15 governmental agencies, large companies and organizations that participate to these
16 surveys, are bound to report losses that must be expressed in million of dollars from
17 laptop theft alone. While the trend is a significant increase from year to year analysts
18 agree to say this is just the tip of the iceberg as most laptop computer thefts go actually
19 unreported. Most stolen equipment is never recovered. Thus, vendors of computer
20 security products have responded with a slew of gadgets to deter laptop theft. As far as
21 physical security is concerned there are many devices available on the market for
22 preventing the theft of equipment. These devices include, locks, cabinets, cables, alarms

1 and deterrent products such as warning labels and equipment used to mark components. If
2 alarms do not prevent the theft of equipment they usually act as a deterrent as well as to
3 alert people in the vicinity or a central location that a device has been removed from its
4 usual location. Alarms can either be installed inside the equipment or on the outside.
5 These devices usually emit loud, piercing sounds if the equipment is moved or if the
6 alarm is tampered with. Some alarms are equipped with keys to enable authorized
7 personnel to deactivate them. Apart from the locks that most personal computers come
8 equipped with, there are other devices that can be used to prevent unauthorized removal
9 of the equipment. Many use either adhesive-mounted pads or metal brackets to fasten the
10 computer and other equipment to a desk or table top. These devices are usually
11 manufactured out of hardened steel. Some use special adhesives and others use bolts.
12 Anchors and cables enable the anchoring of devices to desks. Cables are probably the
13 most common physical security devices and usually the cheapest. They also tend to be the
14 most flexible. Usually, steel cables are passed through metal rings that are attached to the
15 equipment and a desk or table. Although cables prevent an individual from quickly
16 walking away with a piece of equipment, they can be cut, although not with ordinary
17 tools. If all of this is relatively efficient, if indeed properly enforced, it is far to be
18 convenient. Attaching its laptop through a cable to an immovable object every time one
19 moves in its working place is definitively very inconvenient and tend to be often
20 dismissed hence, not really solving the problem.

21 On the other hand laptops used in company and organization offices and workplaces (and
22 even at home which tend to become another workplace) are most often, not to say always,
23 permanently connected to some sort of local area network (wired or wireless) or has a
24 permanent link to an Intranet or an Internet service provider. Because such links are vital
25 to conduct their work and business all those having to use portable computers and similar
26 devices never miss in practice to first connect to their network e.g., to download their
27 mail or to access some sort of data bases to get updated on their business. Hence, the act

1 of connecting to a network is willingly done since it is the necessary step to obtaining the
2 news and information, and to be kept constantly updated, about its everyday activity.

3 SUMMARY OF THE INVENTION:

4 Thus, it is an aspect of the invention to enable surveillance of a network connected
5 device from the network.

6 It is another aspect of the invention to issue an alarm to a central surveillance unit
7 whenever a laptop or similar computer-like device is, without notice, disconnected from a
8 network.

9 It is yet another aspect of the invention to define a log in and log out procedure to permit
10 that a removable computer-like device be reliability monitored while in use and
11 connected to a network.

12 Further aspects, features and advantages of the present invention will become apparent to
13 the ones skilled in the art upon examination of the following description in reference to
14 the accompanying drawings. It is intended that any additional advantages be incorporated
15 herein.

16 Thus the invention provides, methods and system for enabling the surveillance of
17 computer-like devices connected to a communications network. In an example
18 embodiment, a communications network includes a Network Surveillance Server (NSS).

1 Upon joining the communications network, a computer-like device is required to log-in to
2 NSS. Then, NSS polls the device connected on the communications network so that an
3 alarm can be issued from NSS to a central surveillance unit, when the computer-like
4 device fails responding to polling. Prior to leaving the communications network, the
5 computer-like device logs-out from NSS. This allows the computer-like devices to be
6 watched as long as they stay connected onto the communications network

7 BRIEF DESCRIPTION OF THE DRAWINGS

8 These and other aspects, features, and advantages of the present invention will
9 become apparent upon further consideration of the following detailed description of the
10 invention when read in conjunction with the drawing figures, in which:

Fig. 1 illustrates an example of a communications network including a network
surveillance server (NSS) per the invention;

Fig. 2 illustrates the monitoring of devices normally connected to the network at
any moment

Fig. 3 describes the steps of an example of a method according to the invention;
and

Fig. 4 shows alternate and/or supplementary steps to the method of Fig. 3 of the
invention, wherein information is collected about the computer-like
devices and their users and compared to corresponding records in NSS.

11

1 DETAILED DESCRIPTION OF THE INVENTION

2 **Figure 1** illustrates an example context in which the present invention applies. On some
3 sort of network [100] e.g., an IP (Internet protocol) LAN (Local Area Network) i.e.,
4 operated under the TCP/IP suite of protocols, computer-like pieces of equipment are
5 permanently connected while in use. This may include regular desktop PC's as [110], and
6 much frequently in recent years, laptop computers such as [120, 130] and other similar
7 portable devices like a palmtop [125]. Connection to a network as [100] may as well be
8 achieved through a wireless connection [150] so as to reach e.g., a portable phone [140]
9 running the Wireless Application Protocol (WAP) that permits to get access to Internet
10 applications. Alternatively, the whole network may be a wireless network such as a
11 wireless LAN. Then, the invention adds a compulsory service associated to the network
12 [100] and operated, for example, from a network connected server [160] to which any
13 new user must log in [172] whenever it connects. Conversely, when user [170] wants to
14 leave, prior to disconnecting from the network, it must log out [174] first. Hence, this
15 procedure authorizes the surveillance of all connected pieces of equipment connected at
16 some point of time to the network. This is further discussed in following figure. If one
17 device is disconnected, without having normally log out first, an alarm [185] to a central
18 surveillance unit [180] can thus be issued so as all appropriate actions can be taken.

19 **Figure 2** illustrates the monitoring of devices normally connected to the network [200]
20 at any moment. This is done from the server in charge of the surveillance service [260].
21 This latter polls regularly all registered connected devices such as [220]. Depending on
22 the type of network this may have to be accomplished through the activation of various
23 mechanisms. Over an IP network, this can simply be done by issuing a so-called 'PING'
24 command to the device that must be polled i.e., by performing an ICMP (Internet Control
25 Message Protocol) echo request, echo reply test e.g., [265]. The polled device, if still
26 connected, is due to respond. An alternate method for an IP network consists in activating

1 the address resolution protocol (ARP) from the network surveillance server (NSS) [260]
2 so as it can make sure that the polled device is still connected since this latter is due to
3 respond with its Media Access Control (MAC) address which is unique. Thus, the
4 surveillance server manages to interrogate each connected device and obtain a response
5 from it, e.g., as shown in [265] thus, proving that corresponding device [220] is indeed
6 still connected.

7 As far as mobile devices and wireless networks are concerned [240] the question for NSS
8 is rather to understand if device is still in proper hands since this kind of device does not
9 actually physically disconnect from a network (nothing is unplugged) as with a wired
10 LAN. Monitoring may include various methods like checking if mobile stays within a
11 communication cell [242], or a group of cells, it is normally expected to roam in. Also,
12 such a mobile device must identify itself through a portal [250] so, an unexpected use of
13 portal or use of a different portal may become the indication of something that needs to
14 be further checked by NSS before issuing an alarm. And, for those of the portable or
15 mobile devices that are not limited to data only transmission but are normally equipped
16 for transmitting voice and even video too, NSS may house the proper technology to
17 perform biometric checking over the individual [244] actually using the device.
18 Especially, voice intonation can be checked and used as a strong authentication of who is
19 actually using the device.

20 More generally the more sophisticated of the NSS's, per the invention, are devised to not
21 only check if a device is, when applicable, actually physically connected to the network,
22 from which surveillance is exercised, but also to check all sorts of behaving and
23 biometric data about those that are connected and which can be easily acquired through
24 the network itself, like voice and typing speed on a computer keyboard, so as alarms
25 [285] can be timely reported to the surveillance unit [280]. This way of checking, beyond

1 a simple physical disconnection from network, may require to implement further
2 checking by NSS not to trigger false alarms like having to first call back the registered
3 owner [244] of a mobile device for further checking.

4 As far as IP networks are concerned the surveillance service as disclosed by the invention
5 may preferably be implemented in a similar way as the Dynamic Host Configuration
6 Protocol (DHCP) of the Internet Engineering Task Force (IETF) as described in RFC
7 2131, March 1997. While DHCP purpose is to enable individual computers on an IP
8 network to extract their configurations from a server (the 'DHCP' server) that has no exact
9 information about the individual computer that wants to connect until it request this
10 information from the computer itself. At which time this latter is attributed a dynamic IP
11 address for the time of a DHCP lease. Similarly, the invention introduces a NSS or
12 Network Surveillance Server, in charge of watching the computers and devices that desire
13 to connect to the network however, requiring a log in and log out procedure to the
14 network so as they can be watched while connected.

15 **Figure 3** depicts the steps of an example of a monitoring method according to the
16 present invention. It starts when a computer or similar device is joining [300] the network
17 for example by connecting on an Ethernet or Token Ring Local Area Network (LAN).
18 Then, joining computer manages to discover [305] all Network Surveillance Server
19 (NSS) present within the network. This is achieved by methods and techniques known
20 from the art and which depends mainly on the type of network considered. If more than
21 one NSS exist computer must select one NSS server so as it can attempt to log in to it by
22 sending proper credentials [310]. If computer credentials are not accepted log in process
23 is aborted [316]. However, if accepted, NSS may start polling the computer [320]. If
24 computer is no longer found, which is checked at step [325], an alarm is normally issued
25 [326]. This particular step [325] may be more sophisticated than just issuing an alarm at

1 first non responded interrogation. Among numerous possibilities, to be more flexible, the
2 alarm could only have to be issued e.g., after a certain number of interrogations or after
3 some time has elapsed. If found, as normally expected, the next step is to check if user of
4 the computer has requested to disconnect [330] (wants to log out). If not, polling may go
5 on [331] so as to keep watching the device while connected to the network. Polling is
6 preferably done at regular intervals as set with a timer [340] although any other method
7 can be used as well such as random interval polling or polling rate adjustable depending
8 on the number of connected devices and activity observed over the network. If, as
9 checked at step [330], computer user wants however to disconnect it must prove to NSS
10 that it is entitled to do so by providing the proper credentials [350]. If credentials are
11 accepted, the normal case, NSS stops polling the computer [365] so it can be safely
12 disconnected from the network [370]. However, if credentials were not accepted polling
13 goes on [361] so as, if disconnected, this eventually result in the sending of an alarm
14 [326].

15 It is worth mentioning here that 'credentials' broadly refers to any method, known from
16 the art, of authenticating a legitimate registered user. This includes simple methods
17 requiring to sign on and sign off with a password or with a Personal Identification
18 Number (PIN) to much more sophisticated ones e.g., implying the possession and the use
19 of a token or smart card and/or the recognition of biometric data such as finger prints
20 through an appropriate reading device.

21 Also, as already mentioned, the term 'computer' used for illustrating the monitoring
22 method according to the invention must be broadly interpreted as any computer-like
23 device, possibly also handling voice and video, capable of connecting directly or
24 indirectly to a network housing a NSS.

1 **Figure 4** shows alternate or supplementary steps of the monitoring method described in
2 Figure 3 thus, replacing or executed in complement to steps [320, 325]. As already
3 discussed in Figure 2, NSS may also check data it collects about the connected device and
4 its user [422]. This ranges from simple geographic location from where a mobile device
5 is calling [242], to the portal [250] through which it connects, plus some biometric data
6 about at least one authorized user of the device such the typing speed over a key board of
7 a laptop or the voice intonation for a cellular phone or a voice-enabled computer. Hence,
8 the data thus collected through the network, can be compared [427] to what is recorded in
9 NSS for the alleged device and registered user(s) so that, if not matching, an alarm can be
10 issued as well

11 The present invention can be realized in hardware, software, or a combination of
12 hardware and software. A visualization tool according to the present invention can be
13 realized in a centralized fashion in one computer system, or in a distributed fashion where
14 different elements are spread across several interconnected computer systems. Any kind
15 of computer system - or other apparatus adapted for carrying out the methods and/or
16 functions described herein - is suitable. A typical combination of hardware and software
17 could be a general purpose computer system with a computer program that, when being
18 loaded and executed, controls the computer system such that it carries out the methods
19 described herein. The present invention can also be embedded in a computer program
20 product, which comprises all the features enabling the implementation of the methods
21 described herein, and which - when loaded in a computer system - is able to carry out
22 these methods.

23 Computer program means or computer program in the present context include any
24 expression, in any language, code or notation, of a set of instructions intended to cause a
25 system having an information processing capability to perform a particular function

1 either directly or after conversion to another language, code or notation, and/or
2 reproduction in a different material form.

3 Thus the invention includes an article of manufacture which comprises a computer usable
4 medium having computer readable program code means embodied therein for causing a
5 function described above. The computer readable program code means in the article of
6 manufacture comprises computer readable program code means for causing a computer to
7 effect the steps of a method of this invention. Similarly, the present invention may be
8 implemented as a computer program product comprising a computer usable medium
9 having computer readable program code means embodied therein for causing a a function
10 described above. The computer readable program code means in the computer program
11 product comprising computer readable program code means for causing a computer to
12 effect one or more functions of this invention. Furthermore, the present invention may be
13 implemented as a program storage device readable by machine, tangibly embodying a
14 program of instructions executable by the machine to perform method steps for causing
15 one or more functions of this invention.

16 It is noted that the foregoing has outlined some of the more pertinent objects and
17 embodiments of the present invention. This invention may be used for many
18 applications. Thus, although the description is made for particular arrangements and
19 methods, the intent and concept of the invention is suitable and applicable to other
20 arrangements and applications. It will be clear to those skilled in the art that
21 modifications to the disclosed embodiments can be effected without departing from the
22 spirit and scope of the invention. The described embodiments ought to be construed to
23 be merely illustrative of some of the more prominent features and applications of the
24 invention. Other beneficial results can be realized by applying the disclosed invention in
25 a different manner or modifying the invention in ways known to those familiar with the
26 art.